Council of European National
Top-Level Domain Registries

Report on IETF98

Chicago
26-31 March 2017

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

Contents

Highlights

IASA 2.0: Must the IETF re-invent its organisational structure?

10 years after the IETF has broken away from its former secretariat body CNRI and taken over responsibility for administrative functions, the organisation has outgrown the IETF administrative support association (IASA) structure. In this case, "outgrown" does not mean that the organisation has become bigger: it's rather that the set of tasks performed by the administrative structure have become more numerous and also more difficult at times, visa and entrance issues to the US being just the most recent example. A BoF meeting on the possible future of the IASA asked the community if minor adjustments to the current IASA and IAD structures would be enough, or if a greater overhaul of the system was necessary, including a potential change of the IETF's legal nature.

Two important questions loom in the process of another step towards reform for the standards body, initiated by outgoing IETF Chair Jari Arkko: (1) how to reorganise the IETF to move towards taking on organisational control and draw a clearer line between itself and the Internet Society (ISOC), main sponsor and current legal home of the IETF; and (2) how to ensure future stable funding.

Taking back control from ISOC?

The IETF currently still remains an un-incorporated standardisation forum. Therefore, the ISOC provides the legal status necessary for contracting with staff, meeting hotels, sponsors and other service providers.

ISOC Chair Kathy Brown noted in the IASA BoF session that the IETF "wants to be independent, yet sits inside an organisation that has to make decisions dependent on its legal status". Brown did assure participants that the ISOC was prepared to partner with the IETF in the dual effort of potential structural and financial reforms. Yet there seems an unease in parts of the IETF participants about the relationship. There had been questions about how much ISOC staff was involved in what the IAD did, said incoming IETF Chair Alissa Cooper in her outline for the discussions.

The growing list of tasks performed by the ISOC for the IETF falls into two categories. The first one is the more mundane help with financial sustainability of the IETF (with an annual contribution of roughly $2.3 Million USD and support for shortfalls from meetings like the expensive and less-attended Buenos Aires meeting). ISOC staff also supports outreach to sponsors and has put up money for the endowment.

The second category of tasks is the more ephemeral part of developing a more diverse community for the IETF, both geographically and with regard to the stakeholder groups. The ISOC is funding and organising fellowship programs for engineers from developing countries and for regulators. ISOC also sponsors several academic activities: Applied Network Research Paper Award, ACM ISOC Networking Research Workshops and Network and Distributed System Security Workshop, the most recent edition on DNS and Online Privacy, and publishes the IETF Journal.

Given the many programs, but also the fact that ISOC staff is involved in various IETF administrative and practical work, both organisations look glued to one another. Several problems arising from this were brought up during the IASA BoF. Several big sponsors such as Cisco, Comcast and Ericsson made pretty similar statements about the problem to explain why funding went to ISOC when it was the IETF that was actually sponsored. Another issue brought up by Alissa Cooper was that the IETF didn't have "a lot of oversight over the hiring and performance" of staff assigned by ISOC to perform the various tasks for the IETF.

There was even some animosity expressed against ISOC. Randy Bush of IIG called on the IETF to take back things like the outreach program and said "without the IETF, ISOC would not last more than three years". A slight tension seems to surface from that statement over who should be in the driving seat: ISOC, which via the PIR and .org registrations now has considerable financial leeway and has grown to close to 100 staff members, or the non-organisation IETF, which helped to create ICANN (and thereby the domain market).

Surgical operation or clean slate?

One big question posed by several participants in Chicago was if IASA 2.0 should just be an upgrade of the current structure or if a more radical reform was necessary. From the discussions, one can draw the conclusion that there is a trend towards a more substantial solution. Both the outgoing and the incoming IAB Chairs warned about only fixing some holes.

Andrew Sullivan of Oracle-Dyn said that he found that "the structure [is] too weak and needs significant changes". The overburdening of administrative tasks in some positions – for example the IAB Chair – has proved to be a mistake. New IAB Chair Hardie complained that the IAB had lost one of the finest experts on DNS and internationalisation in Andrew Sullivan, as during Sullivan's IAB tenure, he had been overwhelmed with tasks in addition to the large number of IAB Chair ex-officio positions. Trying to fix this structural issue simply by investing more resources would not help, and would be similar to "more people passing data over the wrong API".

Cooper's conclusion from the discussions was that there was "openness to do considerable changes" to the organisational structure. She said she would prepare a strawman paper for discussion. More BoFs and Webinars (as the one in preparation for the IASA BoF) will be held in the coming months.

Concerns about the impact of moving from volunteer to professional

Another concern mentioned by several long-time members of the IETF, including Lucy Lynch, Bob Hinden and Randy Bush, was that the IETF might move from a volunteer-based, self-governed body to a professionally-steered body. An increase in professional staff could result in staff having more influence in how the IETF developed. This goes against the IETF spirit, Lynch said. Pointers were made towards the W3C.

Cooper and several others objected that there was a direct link between more professional staff and loss of self-governance character. Olaf Kolkman (who had presented the numbers on the jobs performed by ISOC for the IETF) said that due to the shift in the industry, the pool of volunteers was dwindling. This makes it difficult to rely solely on volunteers to perform all the necessary tasks to allow for a good IETF experience for developers. Cooper certainly favours a pragmatic approach.

Financial situation: not dire (yet), but action is needed

Arkko was tasked to look into the financial situation. In Chicago, he said that while the financial situation was "not dire, we need to do something about it". He said that the big issue is that payed attendance is only stable while costs are rising. Without higher attendance fees, the meetings' cost and revenues do not match. While the ISOC stepped in for Buenos Aires, the decline of attendance for a US-based meeting was assessed through a special questionnaire on attendees' potential concerns about US visa policy issues.

Change of Chair

In Chicago, Alissa Cooper (Cisco) took over from Jari Arkko (Ericsson) as IETF Chair. Cooper will be the first female Chair of the IETF. While gender diversity clearly has improved in the IETF peer bodies, it was noted by some that there are three Cisco employees on the steering group (IESG): Alissa Cooper, Benoit Claise and Alvaro Retana. For way of comparison, Cisco's direct competitor Juniper has one seat, while Chinese hardware manufacturer Huawei, as well as other potential Asian players, are interestingly absent.

With the US once more being questioned as a meeting space, the fact that all Chair positions at the IETF, IAB and IRTF are held by US-nationals might seem a little unfortunate.

Discussions on the visa issues look like they will continue, as numbers of paid attendance fees for the IETF meeting in Chicago were down (only a few dozen more than the meeting in Buenos Aires). A survey is being circulated to understand if the visa issues could be an ongoing problem. IETF101 is due to be held in San Francisco (more information on these discussions in the "meeting venue WG" section below).

Outgoing Chair Jari Arkko received standing ovations during his farewell party and was portrayed as tireless by his successor Alissa Cooper. Arkko was thrown into the IANA transition and the Snowden fall-out, and had to deal with more policy issues than expected. Arkko is continuing in the role of IAB member.

Should human rights be part of the “tussle”?

The debate about human rights in standardization has turned up a notch: the IETF meeting in Chicago saw a plenary discussion about the ethics of standards-making and the responsibilities for engineers.

Making conflicting interests part of the tussle and trying to tilt the playing field

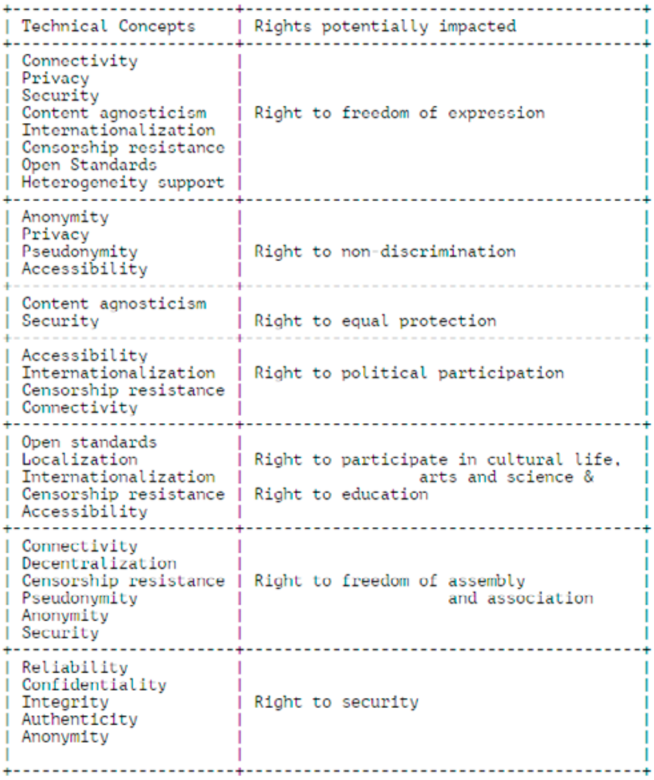
Dave Clark, author of the famous paper on the “Tussle in Cyberspace”, said the most important question for engineers was if they were clever enough to tilt the playing field by shaping the design of their standards (Clark’s plenary presentation can be viewed here). Looking back to the “Raven debate”, Clark highlighted that it resulted in one of the most well-reported decisions by the IETF of a political nature: to reject the standardization of wiretapping from the US CALEA Act. In hindsight, Clark noted, engineers gave up on “tilting the playing field” by not embedding the tussle – the different actors’ conflicting interests – directly into the standard. By refusing to embed law enforcement’s interests and, in a way, shaping how wiretapping would playout inside the standard, they drove law enforcement to different actors with potentially no interest in tilting the playing field.

Another interesting example was mentioned during the discussion by Mike Bishop, a Microsoft engineer and one of the authors of the Quic protocol suite. Bishop pointed out that there was work taken on at the IEEE standards body on multiContext TLS, “a secure communication protocol that extends TLS to allow endpoints to incorporate trusted middleboxes into secure sessions”. Plainly spoken, it is a way to break TLS. Not talking about the tussle of encryption via the interests of network managers or law enforcement and driving these interests away from the IETF resulted in such solutions being prepared elsewhere without even asking the original TLS standardization body for comment on the potential effects.

So while Clark clearly acknowledged the need to talk about human rights in designing technology, bringing social scientists, lawyers and techies together, and said he was supportive of the “value based design movement”, he argued for including divergent interests as much as possible into the design itself.

Human Rights Considerations in Protocols in the IRTF

The IRTF has started down this path with its Human Rights in Protocols Consideration Research Group. Niels ten Oever, Co-Chair of the RG, gave a summary of the work. The HPRC RG has finalized its lengthy document on “Research into Human Rights Protocol Considerations” that attempts to match technical concepts to human rights (see list below) and act as a guideline for designers. Ten Oever called on engineers to consider taking on human rights considerations into the IETF by establishing a Human Rights Working Group.



Technical Concepts	Rights potentially impacted
Connectivity Privacy Security Content agnosticism Internationalization Censorship resistance Open Standards Heterogeneity support	Right to freedom of expression
Anonymity Privacy Pseudonymity Accessibility	Right to non-discrimination
Content agnosticism Security	Right to equal protection
Accessibility Internationalization Censorship resistance Connectivity	Right to political participation
Open standards Localization Internationalization Censorship resistance Accessibility	Right to participate in cultural life, arts and science & Right to education
Connectivity Decentralization Censorship resistance Pseudonymity Anonymity Security	Right to freedom of assembly and association
Reliability Confidentiality Integrity Authenticity Anonymity	Right to security

Reactions to the call for the IETF to talk about human rights when designing were mixed. A smaller fraction taking a position in Chicago argued the IETF might not be the right body due to the lack of expertise (Paul Hofmann, ICANN, Pete Resnick, Qualcom). There were also questions on how the HPRC RFC would be implemented (e.g., Mirja Kühlewind, ETH Zurich). The matching of rights and technical concepts is not clear-cut.

This became clear in the first discussions over new work proposed by ten Oever for the HPRC. In an analogy to the existing “Privacy Considerations” document, ten Oever tabled “something that became clear in starting discussions about new HPRC work on *anonymity* and *freedom of association*". Distributed denial of services, which some activists defended as a potential form of protest years ago, are not in line with freedom of association, ten Oever argued, due to interruption of legitimate traffic, for example.

But despite the reluctance of the IETF participants to engage in the HPRC discussion, most people expressed an understanding that the designers cannot escape addressing possible societal effects of design decisions. "We will tilt the playing field", said former IETF Chair Harald Alvestrand. Engineers can only try to tilt in a conscious manner, without guarantee of being successful. Daniel Kahn-Gilmor from the American Civil Liberty Union underlined that without question, engineers had to address ethics in their work.

Ethical considerations in standards work are quite in fashion lately, with the IEEE running an initiative (see WG and BoFs, HPRC below) and similar efforts in ISO.

New transport protocol Quic advances quickly

Quick standardization is possible, as demonstrated by Quic. The new UDP-based transport protocol developed by Google engineers, which was kept away from IETF standardization in 2014, will be pushed towards the first draft RFC implementation within a year, as confirmed by Lars Eggert, Co-Chair of the Quic Working Group.

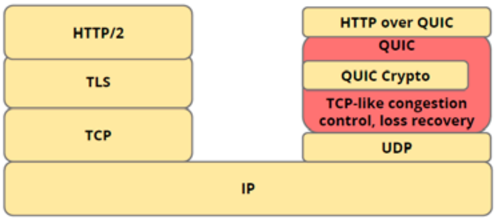
The working group was moving at a "breakneck pace", Google engineer and document author Jana Iyengar said. The WG already had one intersessional meeting in Tokyo in January, will meet again in Paris around June before IETF99 in Prague and plans for a third meeting before IETF100. It is at these intersessional meetings (with 50 participants in Tokyo) that much progress is made, according to observers.

Quic will not only be Google's Quic, underlined Iyengar in a well-attended Quic Tutorial on Sunday before the Chicago meeting. Changes include the header format and the substitution of Google's proprietary encryption with TLS 1.3, which has tried to keep pace with Quic to be ready for the new transport protocol.

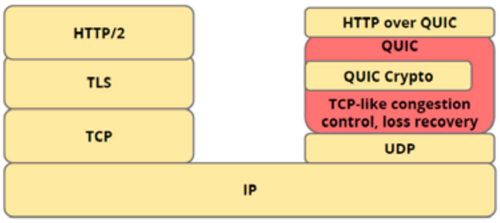
Outgoing IETF-Chair Jari Arkko's comment illustrates well the potential impact of Quic. Arkko said to this reporter that the development of Quic was one of the surprises in his tenure. He had thought that a breakaway from TCP was not possible. Eggert said he expected for Quic to rapidly make up to 60-70 percent of web traffic. Since large browser and software vendors are pushing for Quic (Google, Mozilla, Microsoft), this would happen quickly, Eggert said to this reporter.

Interest has been expressed to work on other than http packets over Quic, for example DNS over Quic. It will be very interesting to see how Quic's success will affect the development of more secure TCP, in TCPinc, but also, if DNS over Quic is standardized, DNS over TLS. There might be work for the privacy advocates in assessing how Quic compared secured TLS versions of traffic.

Old Google QUIC

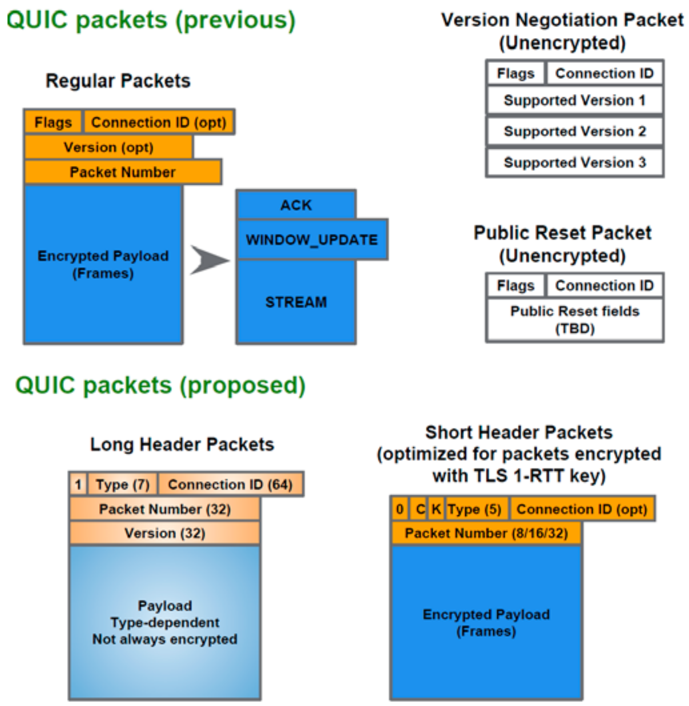


QUIC working group



Header format resolved

Agreement over the Quic header format was a big issue which was resolved before the IETF in Chicago and then presented there.



The new IETF Quic header has two versions: a long header (starting with a "1" bit to indicate it is a long header), a 7 bit type, a 64 bit connection ID and a packet number and version announcement (each 32 bit), plus payload. The long header is used to set up first connections between server and client. The handshake is not encrypted, but authenticated. After the handshake and for connections to a known server, the smaller header format can be used, which only needs five bits type, and up to 32 bit packet number. The Connection ID remains an option. The payload is fully encrypted.

In the original Quic, the version had to be tested; now, the version information is in the header, and while visibility is slightly increased, this was acceptable to authors. The IETF Quic header was now "cleaner", said Iyengar.

Iyengar underlined that the new protocol was reusing a number of existing ideas, TCP Fast Open (T/TCP) and the ongoing TLS 1.3 work, including the faster connection establishment. The 0RTT connection establishment was the major contribution from Quic. To allow for the 0RTT connections, TLS 1.3 introduces sending DiffieHelman parameters and public keys in special *KeyShare* extensions. These are new extension that are embedded in the ServerHello and ClientHello messages. Another reused idea is multiplexed streams over one connection (also used in the TCP based Google developed Speedy).

Middlebox vendors and network operators not amused over encrypted traffic

By reducing header information, Quic reduces "meta data" visibility and tracking options. While TCP information could be scraped from the header fields, Quic is not as handy for that. The discussion about making additional bits visible for trouble-shooting and network management could become the most difficult one, thinks Iyengar.

One proposal by Transport Area Director Mirja Kühlewind (ETH Zurich) is that a number of packet numbers should be echoed back to allow middleboxes passive monitoring. Kühlewind asked for objections against this and some participants warned that stepping back from the possible blurring of connection information should be allowed. Potential privacy issues could be understood in the future, said Daniel Kahn Gilmor, ACLU.

One Quic editor said that intensive talks with middlebox vendors laid ahead, but if the case of the network operators and middlebox vendors did not give ample proof about the problem they had, there was not a lot of incentive for the WG to allow for the additional bits. In line with the tussle question (see above), the WG will have to come to a decision if they reject the requests from the operators and remain more on the privacy side. It looks like a clear-cut test case for HRPC.

home.arpa instead of... .homenet?

In Chicago, opinions about which TLD should be used for the addressing in the homenet were still at odds. That changed with the publication of a brisk statement from the IAB on the difference between special domain reservation (non-DNS use) and special names explicitly intended to work with the DNS (which was declared to need to be under .arpa or another TLD administered by the IAB). A week after the IETF meeting, a new version of the homenet draft was published asking for home.arpa.

In the two weeks before Chicago, IETF participants and ICANN representatives (namely the Chair of the ICANN Board, Steve Crocker) had clashed on the homenet mailing list over the draft proposal to have .homenet not only reserved as a special use TLD, but also delegated in the root zone. Another point of contention also was that the proponents did not want to have the new TLD DNSSEC-signed, as having it signed would result in validation failures due to the local use. With DNSSEC, a validating stub resolver would reject resolving names published under the .home.arpa name server.

What is still unclear at this point in time is how much outside visibility the authors of the homenet architecture want for the home-names.

Talking to this reporter, Ted Lemon, one of the Nominum founders and main proponent of the draft, argued that his understanding of the IETF ICANN MoU clearly allowed for the IETF to initiate such delegations. Lemon particularly pointed to section 4.3 of the MoU (agreed in 2000) that reads

"Note that (a) assignments of domain names for technical uses (such as domain names for inverse DNS look-up), (b) assignments of specialized address blocks (such as multicast or anycast blocks), and (c) experimental assignments are not considered to be policy issues, and shall remain subject to the provisions of this Section 4. (For purposes of this MOU, the term "assignments" includes allocations.) In the event ICANN adopts a policy that prevents it from complying with the provisions of this Section 4 with respect to the assignments described in (a) - (c) above, ICANN will notify the IETF, which may then exercise its ability to cancel this MOU under Section 2 above"

According to Lemon's proposal the IETF should initiate talks with ICANN over the allocation of .homenet – and use it as an opportunity to clear up the disagreements over interpretation.

Lemon's call met with considerable resistance at the Chicago .homenet meeting. The Area Director, Terry Manderson, reminded the WG that asking for an insecure insertion in the root zone was "not covered in IETF policy terms" and "a new process would have to be constructed with ICANN". Outgoing Chair Jari Arkko reminded the WG "to be really clear on what the implications are of some of the requirements", adding that the process could be lengthy. Outgoing IAB Chair Andrew Sullivan (Oracle/Dyn) also warned that opening up the MoU with ICANN might even be disadvantageous to the IETF.

There was considerable critic with regard to the DNSOP dealing with the special names issue. In the end, these warnings resulted in Lemon and his Co-Author Pierre Pfister (Cisco) changing their proposal and going for home.arpa. Lemon did include a slight rant on an issue he has with home.arpa:

"Some service discovery user interfaces that are expected to be used on homenets conceal information such as domain names from end users. However, it is still expected that in some cases, users will need to see, remember, and even type, names ending with '.home.arpa'. It is therefore desirable that users identify the top-level domain and understand that using it expresses the intention to connect to a service that is specific to the home network to which they are connected. Enforcing the fulfilment of this intention is out of scope for this document."

Features retracted from architecture draft

A rather toned down new draft on the naming architecture does not include outside visibility and gives up on other properties planned for in earlier document versions. The new naming architecture does not have a security model, no notion of "state", no clean way to enumerate all services, no place to collect the enumeration of services (mDNS was, Lemon said during the WG, a "flawed protocol" in that sense). mDNS, Lemon said, was not providing a unique identifier per device. Using a heuristic for potential name conflict issues is under discussion, but would allow edge cases.

Lemon said he opted for the slim new naming architecture document to get it advanced. The question for a registration protocol could be solved later in DNSSD, he said. He also said that the WG could still come back with a second document to bring back outside visibility as it was removed from the simple naming draft.

The routing protocol for homenet will be Babel and there was a discussion about how authentication would be done in Babel. While some in the WG said that a mention in the security considerations of the document would suffice, Lemon asked for a threat analysis and a solution to be decided upon. Otherwise, diverse authentication mechanisms would be entertained and interoperability would be lost.

Working Groups and BoFs

RegExt WG: What should come first: standards or policies?

The RegExt WG met twice in Chicago, experimenting with break-out sessions during the first meeting to talk more in depth about proposals on RDAP and EPP. Summaries from the breakouts were presented at a second meeting and the main discussion there was illustrative of a specific problem the group continues to have: in many instances, the group develops mechanisms that are dependent on policy decisions of the stakeholder bodies at ICANN.

The problem is evident in the federated access solution for RDAP queries Verisign has been working on for some time. The solution is based on Open ID Connect (no IETF standard) which allows the registry to make decisions on access based on authentication and validation of third party providers. For VeriSign's test, these were Googlemail, Paypal and Cz.Nic. According to Hollenbeck, the federated access solution can be an option to allow for layered access to third parties like law enforcement and trademark owners. Hollenbeck's description for law enforcement credentials were rather simplistic, though, when he said that validation and accreditation could be outsourced to the FBI. The decision on who is a LEA and who has a legitimate right to access which data is rather tough to solve on a global scale.

Hollenbeck acknowledged that while technologies were working, who should get access to what was currently the topic of a policy development working group at ICANN, "and they are a long way from setting policies". While ccTLD operators might have their guidelines about who gets access to what (with the new EU General Data Protection Regulation being cited as strict in keeping personal data away from public disclosure), anything the RegExt WG would decide upon now "may not be consistent with what ICANN pops out later", Hollenbeck said.

One participant commented that a deadlock should be avoided by the RegExt WG waiting on ICANN, while ICANN potentially saying they could not go ahead due to the lack of a technical standard. The clear question here should be: what should come first – the code or the policy? That question was not asked, however.

Proposals discussed during breakouts and joint meeting

Talking about one of the three RDAP proposals discussed more intensely during the RDAP breakout, Hollenbeck said that the policy work at ICANN on who would receive which data from the new system was still under discussion and would take considerable time.

Scott Hollenbeck (VeriSign) presented all the drafts discussed in the RDAP part of the breakout sessions. There was practically no interest expressed by participants to implement a method to RDAP adding "searchability" using regular expressions. The regularly expression query parameters used were differentiated from core search, and some "coding magic" had to be used because regular expressions were not URL-safe. (The format should support base64url encoding instead of hex encoding to prevent mixing search queries with urls). The result was not command-line-friendly, but was tested by VeriSign against ccTLDs (not gTLDs due to contractual obligations towards ICANN). The solution gave users a "kind Boolean logic", said Hollenbeck. It was possible to do rate limiting, one of the VeriSign developers added, add a stateless enumerator or allow for patches to be sent back (give me the first ten of 100). VeriSign has declared it has IPR on the method, but Hollenbeck said, "it is free code". Searchability has been a controversial issue in discussions over RDAP. As no interest was expressed from attendees, Hollenbeck said he would consider bringing it to the WG as individual submission/informational document (not a standard).

There was also no final agreement on the second proposal, but some interest in working on an "entity tag" allowing for an easier link of service and operator. A convention could be adopted, Hollenbeck said, with some kind of tag that could be pointing to a server. This would build on the existing logic, yet would involve the creation of a IANA registry for the handles. A concern raised here by Marcos Sanz, Denic, was how existing solutions might result in confusion for the clients about where to look and where not to look. At Denic, tags were added as prefix instead of the planned suffix solution, and what would happen if the entity tag would be in the middle. “Strange things might happen”, said Sanz. Discussion will continue on this topic.

The issues discussed during the EPP breakout included a draft on epp fees, a reseller extension (the need was questioned by some, reseller Id is an optional field in the consistent labelling and display policy) and a protocol proposal to allow a third party DNS operator to update DS records for a delegation (a question that was raised was “is this in the scope of the WG?”, the general topic being discussed in earlier meetings DNSOP).

A proposal for new query parameters “availabilityCheck=1” / “availabilityInformation=1” (Andy Newton Arin/Marcos Sanz Denic) resulted in sharp rejection from Jim Gould. RDAP was about information, not availability. Newton offered that different servers could be queried.

Re-chartering: more extension documents – informational or standard track?

The Working Group is about to re-charter (which is necessary to take on the escrow documents, for example). The new area director (and some of the participants) expressed their concerns over the many documents that were processed and approved by a small number of people. So far there doesn’t seem to be a solution for this unfortunate situation.

Co-Chair Jim Galvin (Afilias) – who has been chairing the meetings alone for quite some time now due to the remote participation only of Antoin Verschueren – addressed the critic by announcing he would go through the list of documents in the pipeline to see if they all needed to be standards track or could just become informational documents instead. With many documents now expired, another task was to ask authors to revive and clarify the status. The Escrow documents prepared by ICANN staff (Francisco Arias) also had to be revived.

Published documents: RFC 8056 (RDAP status mapping) plus RFC 8063 (Key Relay). The document for Launch Phase is ready for WGLC (Ulrich Wisser is the group’s Shepard).

DNSOP WG: NSEC5, Special-use TLDs done, .alt on wish list

The DNSOP WG is crunching on a considerable number of documents. With some relief, the Chairs closed the discussions over special domains. The DNS terminology document (WG last call before the Prague meeting) and a document on managing the ip6.arpa zone for IPv6 by Lee Howard (Time Warner Cable) are also close to be finalised.

After the protracted discussion over the special-use TLDs in recent years, the WG Chairs declared consensus, shortly after the IETF meeting, on the document authored by Ralf Droms, Ted Lemon, Nominum, and Warren Kumari, Google. The document is now on its way to the IESG. It distinguishes between five types of names:

- those reserved by the IETF for technical purposes;
- those assigned by ICANN to the public root (of which some names were reserved by the IETF for technical purposes to appear in the Global DNS root for reasons pertaining to the operation of the DNS);
- those reserved by ICANN (for which no applications can be made, for example ccTLDs);
- those used by other organizations (.int,.gov); and
- those unused and available for assignment to one of the categories.

The document also lists the problems with differentiating between the various “types” and gaps in clarity on the procedures for allocation/assignment. It notes, for example, that there is “no existing formal coordination process between the IETF and ICANN as they follow their respective name assignment processes (see Section 4.1.3). The lack of coordination complicates the management of the root of the Domain Namespace and could lead to conflicts in name assignments [SDO-ICANN-SAC090]”. “There is [also] no explicit scoping as to what can constitute a *technical use* [RFC 2860] and what cannot, and there is also no consensus within the IETF as to what this term means”.

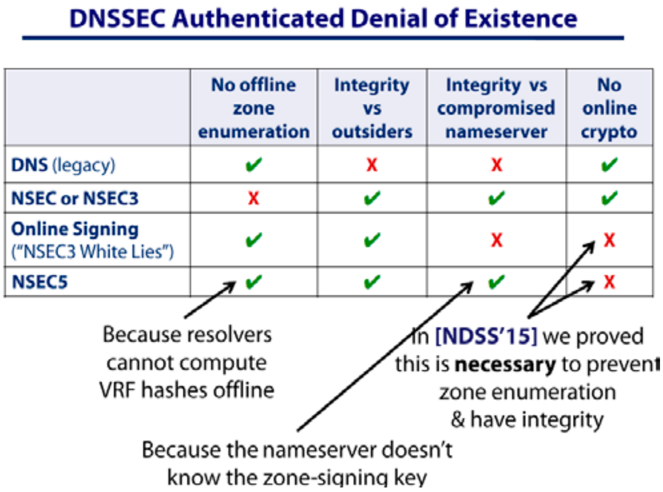
As the new Area Director, Warren Kumari, is an author, it will be assigned to another IESG member for next steps. In the meantime, the proposal to add a .alt su-

TLD as a home for alternative, non-root DNS (home.alt) name arrived in the WG last call, sparking another round of discussion.

NSEC5 is a new proposal brought to the IETF by Crypto expert Sharon Goldberg and authors from cz.nic, Akamai and Salesforce. Goldberg presented the concept in DNSOP and the crypto solution in the security area WG. According to Goldberg, the basic advantage is that it allowed for non-enumeration of zones, combined with integrity protection (against outsider, even when a nameserver was compromised – see graph). The concept would also be viable for high-throughput scenarios, according to Goldberg. In a nutshell, NSEC5 replaces Sha1 with a verifiable random function (vrf). Papers on crypto concept and deployability can be viewed here.

Deployability and necessity of the approach was questioned by participants. Asking DNSSEC implementers to roll back the authenticated denial of existence now would only slow down DNSSEC deployment, some warned. Someone called it an “elegant solution for a problem we don’t have”.

Combination with other concepts like “aggressive use of negative caching” was also questioned.



DNSSEC Authenticated Denial of Existence

	No offline zone enumeration	Integrity vs outsiders	Integrity vs compromised nameserver	No online crypto
DNS (legacy)	✓	✗	✗	✓
NSEC or NSEC3	✗	✓	✓	✓
Online Signing (“NSEC3 White Lies”)	✓	✓	✗	✗
NSEC5	✓	✓	✓	✗

Because resolvers cannot compute VRF hashes offline

In **[NDSS’15]** we proved this is **necessary** to prevent zone enumeration & have integrity

Because the nameserver doesn’t know the zone-signing key

Documents still under development in the group include operational considerations for DNS transport over TCP, capture format for DNS packets (C-DNS) and algorithm update for DNSSEC.

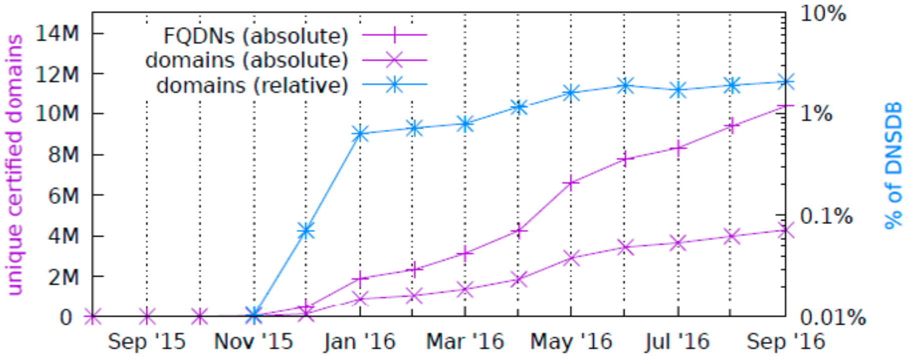
Human Rights Protocol Considerations (HPRC)

The EFF's "Let's encrypt" campaign is a success story, according to a study performed by researchers of the National Cyber Security Center in the Netherlands, Delft University and SIDN Labs and presented during the HPRC Research Group. After the Snowden revelations, the rate of encryption clearly went straight up with reactions in standardization (RFC 7258), and with mobile OS providers and cloud providers pushing encryption by default or enabling it anywhere. Half of the web traffic is now encrypted.

Stats collected by the presenter show that the "Let's encrypt" campaign, which focussed on automation and cheap (free certificates), was much in use by those with less incentive to encrypt – smaller organisations and companies (outside of the Alexa top 100). When mapping the certificates to IP addresses, the study authors found that roughly 66,000 entities have issued certificates with Let's encrypt. What is also interesting is that 47 percent of the growth could be attributed to three large hosting providers.

The HPRC RG was packed with academic presentations which resulted in some debate over the use of meeting time. The two new drafts on anonymity and freedom of association could not be discussed in Chicago. The relation between standardization/engineering and human rights seems to be a rather hot academic topic.

▸ Steady growth



SIDN LABS TUDelft

IETF/IAB noteworthy

IAB prepared for Community Coordination Group (new IANA)

With the IANA transition completed, the IAB has prepared procedures to make appointments for the Community Coordination Group (RFC 8090) and the Root Zone Evolution Review Committee (RFC 8128).

Outgoing and incoming

Ending their terms on the IESG in Chicago were Jari Arkko and Stephen Farrell (Trinity College).

Ending their terms on the IAB were Russ Housely (Vigilsec), Andrew Sullivan (Oracle/Dyn), Ralph Droms and Dave Thaler (Microsoft).

Income 2016 below Budget

The IETF's total 2016 income of $3,925,501 USD was $410,499 USD below budget (-9.5%), while expenditures (excluding Tools Development) totalled $6,354,822 USD, or $147,464 USD less than budgeted. Including the funding of Tools Development, ISOC provided $2,574,164 USD in funding, $208,878 USD above the 2016 budget. The overall outcome was better than was feared in March and was greatly helped by lowering the costs of meeting space and food and beverage due to changes to currency valuation.

Recent IAB reports

Coordinating Attack Response at Internet Scale (CARIS) Workshop Report (at the RFC Editor)

Report from the Internet of Things (IoT) Semantic Interoperability (IOTSI) Workshop 2016

Report from the Internet of Things (IoT) Software Update (IoTSU) Workshop 2016 (in community review, nearly done)

IAB Workshop on Managing Radio Networks in an Encrypted World (MaRNEW) Report

Confidentiality in the Face of Pervasive Surveillance

Out With the Old and In With the New: Planning for Protocol Transitions (in community review, nearly done)

Improving the Public Key Infrastructure (PKI) for the World Wide Web

Incoming and outgoing IETF Chairs Alissa Cooper and Jari Arkko

CENTR is the association of European country code top-level domain (ccTLD) registries, such as .de for Germany or .si for Slovenia. CENTR currently counts 53 full and 9 associate members – together, they are responsible for over 80% of all registered domain names worldwide. The objectives of CENTR are to promote and participate in the development of high standards and best practices among ccTLD registries.

CENTR vzw/asbl
Belliardstraat 20 (6th floor)
1040 Brussels, Belgium
Tel: +32 2 627 5550
Fax: +32 2 627 5559
secretariat@centr.org
www.centr.org

To keep up-to-date with CENTR activities and reports, follow us on Twitter, Facebook or LinkedIn